Information Security Plan

Agency:

Date:

Contact:

TABLE OF CONTENTS

Introduction 1
Terms and Definitions 1
Authority 2
Roles and Responsibilities 2
Security Program 3
Security Components 4
- Risk Management 4
- Security Policy 5
- Organization of Information Security 5
- Asset Management 5
- Human Resources Security 6
- Physical and Environmental Security 6
- Communications and Operations Management 6
- Access Control 7
- Information Systems Acquisition, Development and Maintenance 7
- Information Security Incident Management 8
- Business Continuity Management 8
- Compliance 8

Implementation 9
Approval 10

Introduction

Note to agencies – This security plan template was created to align with the ISO 27002:2005 standard and to meet the requirements of the statewide Information Security policy. Agencies should adjust definitions as necessary to best meet their business environment.

Information is an asset that, like other important business assets, is essential to an organization's business and consequently needs to be suitably protected. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or by using electronic means, shown on films, or spoken in conversation. In whatever form the information takes, or means by which it is shared or stored, it should always be appropriately secured.

Information security is the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities. Information security is achieved by implementing a suitable set of controls, including policies, processes, procedures, organizational structures, and software and hardware functions. These controls need to be established, implemented, monitored, reviewed and improved, where necessary, to ensure that the specific security and business objectives of the organization are met. This should be done in conjunction with other business management processes.

The objectives identified in this plan represent commonly accepted goals of information security management as identified by the ISO/IEC 27002:2005 *Information technology – Security techniques – Code of practice for information security management*, the recognized standard for Oregon state government. The plan is created and managed in accordance with the provisions of Oregon Revised Statute 182.122 and Oregon Administrative Rules 125-800-005 through 125-800-0020.

Terms and Definitions

Note to agencies – These definitions come from the ISO 27002:2005 standard and are presented here simply as an example. Agencies should adjust definitions as necessary to best meet their business environment.

asset	anything that has value to the agency
control	means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature
information security	preservation of confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved
policy	overall intention and direction as formally expressed by management
risk	the likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact
risk assessment	overall process of risk analysis and risk evaluation
risk evaluation	process of comparing the estimated risk against given risk criteria to determine the significance of the risk
risk management	coordinated activities to direct and control the agency with regard to risk

threat	a potential cause of an unwanted incident, which may result in harm to a system or the agency
vulnerability	a weakness of an asset or group of assets that can be exploited by one or more threats

Authority

Statewide information security policies:

Policy Number	Policy Title	Effective Date
107-004-050	Information Asset Classification	1/31/2008
107-004-051	Controlling Portable and Removable Storage Devices	7/30/2007
107-004-052	Information Security	7/30/2007
107-004-053	Employee Security	7/30/2007
107-004-100	Transporting Information Assets	1/31/2008
107-004-110	Acceptable Use of State Information Assets	10/16/2007
107-004-xxx	Information Security Incident Response	draft

<agency> information security policies:

Policy Number	Policy Title	Effective Date

Roles and Responsibilities

Note to agencies – These role descriptions come from the statewide information security policies and are presented here simply as an example. Agencies should adjust these descriptions as necessary to best meet their business environment and include any additional roles that have been identified in the agency that apply such as Security Officer, Privacy Officer, etc.

Agency Director — Responsible for information security in the agency, for reducing risk exposure, and for ensuring the agency's activities do not introduce undue risk to the enterprise. The director also is responsible for ensuring compliance with state enterprise

	security policies, standards, and security initiatives, and with state and federal regulations.
Incident Response Point of Contact	Responsible for communicating with State Incident Response Team and coordinating agency actions in response to an information security incident.
Information Owner	Responsible for creating initial information classification, approving decisions regarding controls and access privileges, performing periodic reclassification, and ensuring regular reviews for value and updates to manage changes to risk.
User	Responsible for complying with the provisions of policies, procedures and practices.

Security Program

Information security is a business issue. The objective is to identify, assess and take steps to avoid or mitigate risk to agency information assets. Governance is an essential component for the long-term strategy and direction of an organization with respect to the security policies and risk management program. Governance requires executive management involvement, approval, and ongoing support. It also requires an organizational structure that provides an appropriate venue to inform and advise executive, business and information technology management on security issues and acceptable risk levels.

<detail on agency governance structure – identify who is responsible for managing information security for the agency, who is responsible for developing policy, who is responsible for assessing risk, who has the authority to accept risk, who is responsible for awareness, identification of any governing bodies such as management committees and work groups, etc. Include other related program areas such as business continuity planning, risk management, and privacy.>

In order to implement and properly maintain a robust information security function, <agency> recognizes the importance of:

- Understanding <agency's> information security requirements and the need to establish policy and objectives for information security;
- Implementing and operating controls to manage <agency's> information security risks in the context of overall business risks;
- Ensuring all users of agency information assets are aware of their responsibilities in protecting those assets;
- Monitoring and reviewing the performance and effectiveness of information security policies and controls; and
- Continual improvement based on assessment, measurement, and changes that affect risk.

<detail agency information security goals including, where applicable, ties to business continuity planning, risk management, audit and assessment, and privacy>

Security Components

Risk Management

Risk Management refers to the process of identifying risk, assessing risk, and taking steps to reduce risk to an acceptable level. Risk management is critical for <agency> to successfully implement and maintain a secure environment. Risk assessments will identify, quantify, and prioritize risks against agency criteria for risk acceptance and objectives. The results will guide and determine appropriate agency action and priorities for managing information security risks and for implementing controls needed to protect information assets.

Risk management will include the following steps as part of a risk assessment:

1. Identify the risks
    a. Identify agency assets and the associated information owners
    b. Identify the threats to those assets
    c. Identify the vulnerabilities that might be exploited by the threats
    d. Identify the impacts that losses of confidentiality, integrity and availability may have on the assets
2. Analyze and evaluate the risks
    a. Assess the business impacts on the agency that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of those assets
    b. Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented
    c. Estimate the level of risks
    d. Determine whether the risks are acceptable
3. Identify and evaluate options for the treatment of risk
    a. Apply appropriate controls
    b. Accept the risks
    c. Avoid the risks
    d. Transfer the associated business risks to other parties
4. Select control objectives and controls for the treatment of risks

It is recognized no set of controls will achieve complete security. Additional management action will be implemented to monitor, evaluate, and improve the efficiency and effectiveness of security controls to support agency goals and objectives.

[ORS 182.122 requires agencies to conduct vulnerability assessments through self assessments, third party contractors, or, as resources are available, DAS through its Enterprise Security Office. The purpose of these assessments is to review/verify security of information systems. Agencies are required to provide assessment and audit results to the Enterprise Security Office.]

<detail on agency risk management structure – this should include roles and responsibilities for the steps involved in risk assessment, identification of a risk assessment methodology or minimum requirements/components, identification of those with the authority to acceptor transfer risks, and steps to be taken to meet the requirements of ORS 182.122.>

<detail agency risk management objectives and initiatives>

Security Policy

The objective of information security policy is to provide management direction and support for information security in accordance with <agency> business requirements and governing laws and regulations. Information security policies will be approved by management, and published and communicated to all employees and relevant external parties. These policies will set out <agency> approach to managing information security and will align with relevant statewide policies.

Information security policies will be reviewed at planned intervals *<insert interval here, i.e. annually>* or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness. Each policy will have an owner who has approved management responsibility for the development, review, and evaluation of the policy. Reviews will include assessing opportunities for improvement of <agency's> information security policies and approach to managing information security in response to changes to <agency's> environment, new threats and risks, business circumstances, legal and policy implications, and technical environment.

[ORS 182.122 requires agencies to develop and implement policies and procedures based on enterprise-level policies.]

<detail agency security policy objectives and initiatives>

Organization of Information Security

Information security will be managed within <agency>. Management will approve information security policies, assign security roles, and coordinate and review the implementation of security across the agency. Information security will be coordinated across different parts of the agency with relevant roles and job functions. Information security responsibilities will be clearly defined and communicated. Security of <agency's> information assets and information technology that are accessed, processed, communicated to, or managed by external parties will be maintained.

<detail agency organizational objectives and initiatives, including information security management structure, governance, etc.>

Asset Management

The objective of asset management is to achieve and maintain appropriate protection of <agency> assets. All agency assets will be identified. Owners of information assets will be identified and will have responsibility for identifying the classification of those assets and maintenance of appropriate controls. To ensure information receives an appropriate level of protection, information will be classified to indicate the sensitivity and expected degree of protection for handling. Rules for acceptable use of information and information assets will be identified, documented, and implemented.

<This will likely be the largest component of the agency plan and it has ties to several statewide policies such as information asset classification, transporting information assets, and securing information assets. Detail agency asset management objectives and initiatives, processes to identify information assets and information owners, determine information sensitivity and classification, and risk assessment processes. Identify processes for determining appropriate levels of protection for information assets based on their sensitivity and classification. See requirements in the statement Information Asset Classification policy, #107-004-050. Include citation for legislation, regulations, policy compliance and/or contractual

obligations that affect management of the information (such as HIPAA, IRS regulations, etc.). If processes are laid out in agency policy, cite policy and attach a copy as an appendix.>

Human Resources Security

All employees, volunteers, contractors, and third party users of <agency> information and information assets will understand their responsibilities and will be deemed suitable for the roles they are considered for to reduce the risk of theft, fraud or misuse. Security responsibilities will be addressed prior to employment in position descriptions and any associated terms and conditions of employment. Where appropriate, all candidates for employment, volunteer work, contractors, and third party users will be adequately screened, especially for roles that require access to sensitive information. Management is responsible to ensure security is applied through an individual's employment with <agency>.

<discuss background checks, drug testing, financial screening, use of confidentiality or non-disclosure agreements, signing of policies, information to be included in job descriptions, information to be reviewed during evaluations, etc.>

All employees and, where relevant, volunteers, contractors and third party users will receive appropriate awareness training and regular updates on policies and procedures as relevant for their job function.

<Discuss training programs, cycle/schedule, etc. Identify security awareness and training elements – topics to be covered, who will be trained, how much training is required.>

Procedures will be implemented to ensure an employee's, volunteer's, contractor's or third party's exit from <agency> is managed and the return of all equipment and removal of all access rights are completed.

<detail agency human resources security objectives and initiatives>

Physical and Environmental Security

The objective of physical and environment security is to prevent unauthorized physical access, damage, theft, compromise, and interference to <agency's> information and facilities. Locations housing critical or sensitive information or information assets will be secured with appropriate security barriers and entry controls. They will be physically protected from unauthorized access, damage and interference. Secure areas will be protected by appropriate security entry controls to ensure that only authorized personnel are allowed access. Security will be applied to off-site equipment. All equipment containing storage media will be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal in compliance with statewide policies.

<discuss key card systems, badge requirements, guidelines, disposal and re-use requirements, etc.>

<detail agency physical security objectives and initiatives>

Communications and Operations Management

Responsibilities and procedures for the management and operation of all information processing facilities will be established. As a matter of policy, segregation of duties will be implemented, where appropriate,

to reduce the risk of negligent of deliberate system or information misuse. Precautions will be used to prevent and detect the introduction of malicious code and unauthorized mobile code to protect the integrity of software and information. To prevent unauthorized disclosure, modification, removal or destruction of information assets, and interruption to business activities, media will be controlled and physically protected. Procedures for handling and storing information will be established and communicated to protect information from unauthorized disclosure or misuse. Exchange of sensitive information and software with other agencies and organizations will be based on a formal exchange policy. Media containing information will be protected against unauthorized access, misuse or corruption during transportation beyond <agency's> physical boundaries.

<Discuss restrictions related to use of portable and removable storage devices, procedures for handling and storing sensitive information, procedures for exchanging information, procedures for transporting information, etc. See requirements for Asset Management section of the security plan.>

To detect unauthorized access to agency information and information systems, systems will be monitored and information security events will be recorded. <agency> will employ monitoring techniques to comply with applicable statewide policies related to acceptable use.

<detail agency communications and operations management objectives and initiatives>

Access Control

Access to information, information systems, information processing facilities, and business processes will be controlled on the basis of business and security requirements. Formal procedures will be developed and implemented to control access rights to information, information systems, and services to prevent unauthorized access. Users will be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords. Users will be made aware of their responsibilities to ensure unattended equipment has appropriate protection. A clear desk policy for papers and removable storage devices and a clear screen policy will be implemented, especially in work areas accessible by the public. Steps will be taken to restrict access to operating systems to authorized users. Protection will be required commensurate with the risks when using mobile computing and teleworking facilities.

<password policies, policies/procedures around access to systems (who controls it, the right to revoke access, etc.), best practice/policy for locking systems when not in use, use of automatic time-out feature on screen savers, clear desk/clear screen policies, telework policy, etc.>

<detail agency access control objectives and initiatives>

Information Systems Acquisition, Development and Maintenance

Policies and procedures will be employed to ensure the security of information systems. Encryption will be used, where appropriate, to protect sensitive information at rest and in transit. Access to system files and program source code will be controlled and information technology projects and support activities conducted in a secure manner. Technical vulnerability management will be implemented with measurements taken to confirm effectiveness.

[ORS 182.122 states that agencies are responsible for information security and security of their systems, applications, desktop, LANS, etc. The State Data Center is given explicit authority over security of the state network and systems within State Data Center control.]

<This is IT-driven. Input is needed from IT group in the agency. Include such things as policies regarding use of encryption, reference to security in system development lifecycle methodologies, vulnerability assessment and penetration testing etc. Include steps to be taken to meet the mandate of ORS 182.122>

<detail agency acquisition, development and maintenance objectives and initiatives>

Information Security Incident Management

Information security incidents will be communicated in a manner allowing timely corrective action to be taken. Formal incident reporting and escalation procedures will be established and communicated to all users. Responsibilities and procedures will be established to handle information security incidents once they have been reported.

[ORS 182.122 requires agencies to develop the capacity to respond to incidents, including implementation of forensic techniques, implementation of remedial actions, and evaluation of lessons learned. Statute also requires agencies report incidents and planned actions to DAS through its Enterprise Security Office.]

<agency plan to comply with statewide incident response policy (still in draft); designated point of contact for incident reporting for the agency; point to incident response plan; detail process for required reporting; and steps to be taken to meet the mandates of ORS 182.122. >

<detail agency information security incident management objectives and initiatives>

Business Continuity Management

The objective of business continuity management is to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption. A business continuity management process will be established to minimize the impact on <agency> and recover from loss of information assets to an acceptable level through a combination of preventive and recovery controls. A managed process will be developed and maintained for business continuity throughout the agency that addresses the information security requirements needed for <agency's> business continuity.

<pointer to agency BCP plan, etc.>

<detail agency business continuity management objectives and initiatives, including review and revision cycles and testing schedules>

Compliance

The design, operation, use, and management of information and information assets are subject to statutory, regulatory, and contractual security requirements. Compliance with legal requirements is necessary to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements. Legal requirements include, but are not limited to: state statute, statewide and

agency policy, regulations, contractual agreements, intellectual property rights, copyrights, and protection and privacy of personal information.

<list policies (statewide and agency), federal regulations, statutes, administrative rules that apply, etc.>

Controls will be established to maximize the effectiveness of the information systems audit process. During the audit process, controls will safeguard operational systems and tools to protect the integrity of the information and prevent misuse.

<identify internal audit roles and responsibilities re: information security, including audit of information systems and associated applications, business processes, etc.>

<detail agency compliance objectives and initiatives>

Implementation

[OAR 125-800-0005 through 125-800-0020 requires agencies to developing an information security plan based on the enterprise standard (as laid out in ORS 182.122, the cite OAR, and published statewide policy. Agencies are to submit security plans to the DAS Enterprise Security Office for certification and revise plans to meet certification requirements.]

<summary of initiatives, tactical plans and implementation initiatives to meet plan components, including timelines, performance measures, auditing/monitoring requirements for compliance, etc. >

Approval

<approval sign off by agency decision makers, i.e. agency administrator, security officer, CIO, etc.>

By: _____ _____
Name, title Date

By: _____ _____
Name, title Date

By: _____ _____
Name, title Date